COVER SHEET

ENTERPRISE MANAGEMENT SYSTEMS: USAGE, AUDIT, AND CONTROL ISSUES

Peter F. Green

University of Queensland,
UQ Business School
Ipswich QLD 4305, Australia
p.green@business.uq.edu.au

Peter Best

Queensland University of Technology, School of Accountancy
Brisbane QLD 4000, Australia
p.best@qut.edu.au

Marta Indulska

University of Queensland,
UQ Business School
Ipswich QLD 4305, Australia
m.indulska@business.uq.edu.au

Abstract

Today, organisations may have production applications running on tens, even hundreds of servers, spread geographically throughout the organisation. In such an environment, organisations cannot rely entirely on human operators/administrators. Moreover, the organisation needs centralised control over the operation of these corporate servers. In such circumstances, organisations will look to software assistance through packages collectively known as Enterprise Management Systems (EMS). The main objective of this study is to identify, based on survey responses, the extent of use of EMS products in Australian organisations as well as identify the functionality used and the critical issues that arise from the introduction of EMS products. While the survey showed that over 50% of responding Australian organizations did not utilise EMS products, the remaining respondents identified operating system management, standardised reporting and user notification as the most frequently used EMS functionality. Furthermore, among the many identified issues that arise when EMS is introduced, multiskilling staff and lack of qualified staff were the most frequent obstacles to EMS utilisation. The results obtained through the administration of the survey are also compared with the results obtained from a previous study of five large organisations.

Keywords: *Enterprise Management Systems, Lights Out Operation, IS Audit and IS controls.*

ENTERPRISE MANAGEMENT SYSTEMS: USAGE, AUDIT, AND CONTROL ISSUES

1 INTRODUCTION

Today, modern businesses are running their corporate applications across many servers linked by local and wide area networks (Ayers & Fentress, 2000; Gisinger *et al*, 2001). The operational management of those core applications, servers, and networks is complicated significantly by the geographical distances that may be involved. Furthermore, the cost of operational management of these corporate resources is likewise significantly increased. Just as technology has been applied to obtain efficiencies in normal business processes, it has been applied progressively over the last decade to achieve efficiencies and operational goals in the management of such corporate computing facilities. Early versions of these hardware and software tools used to automate computing operations were called automated operator facilities (AOF) (or, "lights out" operations). These solutions focused on automating the backup/restart procedures and responding to system alerts. Today, such solutions are called enterprise management systems (EMS) and they incorporate such an array of functionality so as to allow the complete management of disparate corporate facilities from one centrally controlled location.

The usefulness of AOF/EMS operations has been apparent in North American sites since the late 80's (Miller, 1988; King, 1990; Greenstein, 1992; Mullen, 1993; Sprague & McNurlin, 1993; Marlin, 1999; Gisinger *et al.*, 2001). The cost-effectiveness, and hence the take-up, of technological innovations in Australian sites tends to lag its North American counterparts by some five to seven years usually. Factors such as proven productivity gains, increased labour award flexibility allowing significant labour reductions in the operations area, a significant increase in the number of EMS products on the market and a commensurate drop in the cost of EMS hardware and software have all combined to bring about a marked increase in the use of EMS operations (to varying degrees) in Australian computer centres. To date, however, there does not appear to be any evidence on the degree of pervasion and the major products used in Australia. Furthermore, the replacement of human operators with automated solutions to control some (or all) of the corporate computing operational tasks in several disparate sites throughout organisations has led to a whole new range of control issues that to date have received little attention in the academic literature, and even less attention in the practitioner literature (CISA Review Manual, 2004; Weber, 1999).

Accordingly, the research presented in this paper is motivated in several ways. First, we want to obtain empirical data indicating the extent of the use of EMS products in Australian based organisations as well as find out what the most frequently used products are. Second, we want to find out what functional capabilities of EMS are being popularly utilised. Third, we want to provide internal, external, and IS auditors with empirically based guidance on controls for these AOF/EMS environments. Moreover, we want this guidance to be founded on, not so much "best practice", but, of the "best practice", which controls are found to be cost-effective, and therefore, utilised currently in practice. Finally, we were motivated to perform this study in order to contribute to the academic literature on what critical audit and control issues arise when an organisation uses EMS.

In order to gather such information, an empirical study utilising a mail-out survey was designed. The collective goal of the survey questions was to determine what types of EMS were used, as well as

what functional capabilities were utilised and what controls were in place over the EMS. The survey also collected data on any additional issues that arose due to the use of EMS products. In summary, we found that, currently, usage of EMS is not as extensive as was suggested originally. Less than 50% of respondents were, at the time of the survey, utilising EMS products. Based on the respondents who indicated EMS usage, the most popular end-to-end EMS products were found to be: BMC Patrol, HP Openview, IBM Tivoli, CA Unicentre and Sophos. Moreover, EMS products, in general, were utilised mostly for operating system management, standardized reporting and user notification, while the usage of other EMS functionality was relatively low. Furthermore, the survey data indicates organisations implementing AOF/EMS appear to pay little attention to the control issues of separation of duties (*i.e.*, different people/groups developing, maintaining, and migrating scripts/parameters) and producing/changing scripts according to organisational standards. Mediocre attention is paid to the implementation of change controls for scripts, establishing/maintaining scripts and parameters in secure libraries, and establishing/maintaining authorisation procedures for the production/changes to scripts. By contrast, significant attention is paid to the establishment of backup procedures for the scripts, contingency plans in the event the EMS fails and interrupts the operation of the entire production system, and documentation about the scripts and their use. In addition, to these *a priori* control issues, multiskilling staff, a lack of qualified/motivated staff, outsourcing due to a lack of internally qualified staff, and the pace of technology/business change that influence the systems we are attempting to control, are the top four issues that respondents believe also need to be controlled in the implementation of AOF/EMSs.

The remainder of this paper unfolds in the following manner. The next section provides a brief introduction to enterprise management systems and the functionality they provide to an organization. The third section reviews prior related work and the controls that are thought to be required when utilising EMS. Section four presents the research methodology used in this study. The fifth section provides the quantitative results of the survey as well as a comparison of the results to a previous study involving interviews of five local organisations (Green & Best, 2003). Finally, the last section summarises the work and limitations of this study.

2 ENTERPRISE MANAGEMENT SOFTWARE AND FUNCTIONALITY

A wide range of enterprise management software (EMS) products is available for automating various aspects of the management of an organisation's information systems. These products may be designed for the mainframe or client/server environments, and may represent solutions for specific tasks, *e.g.*, storage management, or provide "end-to-end" solutions incorporating the vendor's own specialised products and/or those of other vendors. Examples of specialised products are Legato Storage Manager, Axent Software's OmniGuard™ security management software and Seagate's Backup Exec™ software management solution. Examples of end-to-end solutions are IBM's Tivoli Management Environment (TME) ® 10, Computer Associates' Unicenter TNG ®, Hewlett-Packard's OpenView ®, BMC's Patrol ®, Aprisma's (Cabletron's) Spectrum ®, Candle Corporation's MQ Series and BullSoft's EMS package (Ayers & Fentress , 2000).

Garvey (1999), Hagendorf-Follett (2001), Lais (2000a), Lais (2000b), Middlemiss (2000), Saunders (1999), Songini (2000), and Yasin (1999) explain that the key capabilities provided by EMS products include:

- Automatic detection of applications, databases and hardware environment, including desktops, network computers, hubs, routers and internet gateways.
- Graphical presentation of topology, business process views and floor plans.
- Standardised reporting including system performance metrics.

- Automating production setup, scheduling, execution and monitoring of processes.
- Job restart. Job restart systems can analyse why jobs terminate abnormally and automate restart and recovery processes.
- User notification system to provide an alert notification facility that notifies users of anomalous events.
- Active server-based virus scanning at the point of entry for e-mails and their attachments, and the monitoring of shared folders.
- EMS products can monitor a range of database availability issues, including backup server, table spaces, logs, locks, cache, file backup status and transaction queues.
- Operating system management that includes automatic discovery and continuous monitoring support for the operating system across a LAN or WAN, monitoring key components – CPU, memory, disks, network communications, processes, users, disk I/O, and queues.
- Application management that involves central monitoring and management of applications and services for peak performance and availability. Organisations spend millions of dollars on enterprise resource planning (ERP) systems like SAP R/3, services and infrastructure. An EMS product can utilise various components to monitor the ERP system, execute certain tasks in response to system alerts, and deploy the graphical user interface (*e.g.*, SAPGUI) to large numbers of desktops.
- Automated monitoring and management of internet services for UNIX and Windows NT.
- Job flow and workload management.
- Network management that includes event, fault, configuration, and performance management of networks. This service ensures the LANs run smoothly, with minimal network downtime. The EMS monitors and analyses WAN traffic, and manages interfaces between local and backbone networks.
- EMS products may provide comprehensive security management through authentication, access control, encryption, and audit trail analyses across multiple platforms.
- Storage management that includes backup, encryption, compression, version and time control, vaulting, and robotics; and
- Resource accounting and charging based on the tracking of usage of resources by user and cost centre, and determine charges.

Recent developments in EMSs incorporate predictive analysis modelling capabilities. For example, Computer Associates' Neugents ™ software used in Unicenter TNG monitor systems for unusual patterns and behaviour in real time and can analyse historical performance data to provide the ability to create a model of a system's patterns and predict future activity. BMC's Patrol ™ incorporates predictive analysis and capacity planning software for advanced modelling and analysis of changes in hardware, applications and transaction rates (see for example, Johnston, 2001, and Yasin, 2000).

3 PRIOR RELATED WORK

When an information system is a prominent part of an organisation's internal control environment, Auditing Standard AUS 214 (.02) and its American equivalent, SAS 94 (20), clearly dictate that the auditor should consider how the IS environment affects the audit. Accordingly, the control objectives and control procedures have to be translated into IS-specific control objectives and procedures. This task has been done comprehensively over the years by the auditing standard setters, academic, and

practitioner literatures (see for example, AUS 412 (.14); AUS 402 (.19 (e)); SAS (19); Weber, 1999; Bae *et al.*, 2003; CISA Review Manual, 2004). In particular, Weber (1999) and the CISA Review Manual (2004) give good guidance on the IS control procedures required in an IS environment. They categorise them as general management controls and application specific controls. The general management controls include controls over general organisation and management, access to data and programs, systems development methodologies and change control, data processing operations, systems programming and technical support, data processing quality assurance procedures, physical access, back-up, and recovery planning. The application specific controls look at controls over input, processing, output, network communications, and databases for each major application system.

In particular, in programmed environments, authors such as Weber (1999) and Bae *et al.* (2003) point out that the highly pertinent general controls are separation of duties, security over access to the source and object code versions of the programs and their parameters, development standards (*i.e.*, programs developed in an authorised manner), change control for the programs, and, back-up and recovery procedures.

Due to the introduction of EMS to organisations, the extent of human intervention by operators has been minimised and, accordingly, the nature of the auditor's general control review of the operations area has also changed dramatically. In effect, by implementing EMS/AOF operations, organisations are replacing predominantly human-controlled environments with programmed environments as the EMS/AOF systems consist of hardware controlled by program scripts written using languages specific to the products. Accordingly, the control procedures specific to programmed environments, tailored to the characteristics of EMS/AOF systems, become more relevant.

Weber (1999) and King (1990) provide a limited review of the controls thought to be needed in this area, at least according to the prescriptive academic IS audit literature. These researchers prescribe that the important audit issues that need to be investigated, clarified, and detailed are:

1. Authorisation of the design, implementation, and maintenance of EMS/AOF programs (procedures or parameters).
2. Separation of duties between the people who write the EMS/AOF procedures and those people who install the procedures in the EMS/AOF hardware.
3. Storage of the EMS/AOF procedures and the security over that storage.
4. The extent to which the EMS/AOF procedures can interfere with the running of production application systems; for example, being able to suppress, not allow to be logged, or ignore application system error messages.
5. Documentation of EMS/AOF procedures.
6. Back-up and off-site storage of EMS/AOF programs, parameters.
7. Contingency plans for the failure of EMS/AOF hardware and/or software.

Furthermore, the Certified Information Systems Auditor (CISA) review manual (2004, p. 166) identifies briefly some concerns that arise in an automated systems management environment. "These include:

1. Remote access to a master console is often granted to stand-by operators for contingency purposes such as automated software failure. Therefore, communication access is opened to allow for very risky, high-power, console commands. Communication access security must be extensive. This would include using leased lines and dial-back capabilities.
2. Contingency plans must allow for the proper identification of a disaster in the unattended facility. In addition, the EMS/AOF controlling software or manual contingency procedures must be adequately documented and tested at the recovery site.

3. The application of proper program change controls and access controls, because vital IS operations are performed by software systems. Also, tests of software should be performed on a periodic basis especially after changes or updates are applied.
4. Assurance that errors are not hidden by the software and that all errors result in operator/network administrator notification."

These issues from the literature are summarised in Figure 1 below.

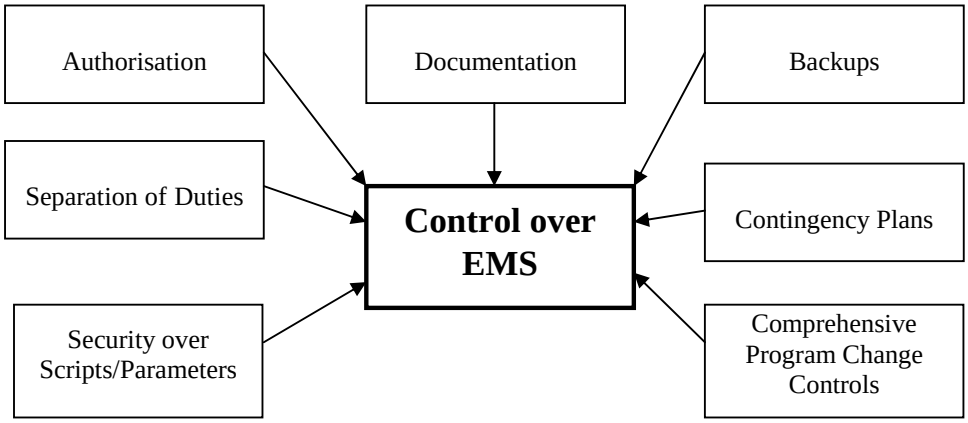

Figure 1. Prescribed general controls over EMS.

To date however, little empirical verification of these prescribed controls has been conducted. Accordingly, while auditors have some "best practice" guidelines normatively stated in the literature, they do not have any guidance on whether these are all of the general control issues critical to EMS environments, or indeed, which may be deemed by practice to be cost-effective and therefore used. Green and Best (2003) conducted a qualitative study on these concerns. Their research involved in-depth semi-structured interviews with five large organisations that had implemented some form of EMS. They found that the prescriptive IS Audit academic and practitioner literatures are deficient still with regard to critical issues such as the level of operating system privilege at which this type of software operates, the presence of an adequate level of expertise in the software at the site, and the presence of an adequate level of backup for the critical human experts in this type of software. Moreover, even though sites are aware of many of the critical audit issues prescribed in the literature, they appear to pay no/little attention (on average) to several of these issues, *e.g.*, authorisation of the development/maintenance of scripts, separation of duties, remote access to master consoles, documentation of scripts and design decisions, and change controls. Furthermore, there were control issues of which the participants made no mention at all, *viz.*, developing scripts according to authorised standards, maintenance of current off-site copies of scripts, and ensuring errors are not hidden by the executing scripts. Indeed, only secure file storage of the parameters/scripts, and ongoing monitoring over the adequacy and completeness of EMS/AOF operations appear to attract high levels of attention at sites. However, the Green and Best (2003) study was preliminary and therefore limited in scope. Only five organisations in one major metropolitan area were included.

4 METHODOLOGY

This study was conducted in the form of a survey[1] mailed-out to organisations Australia-wide. The participants were selected from the *MIS 4000* database obtained from the Strategic Publishing Group Pty Ltd in 2002. This database contained demographic information on 4000 IS installations within organisations throughout Australia and New Zealand. This information included, *inter alia*, the name and address of the CIO and the size of the organisation in terms of the number of employees and the number of online terminals. Because we suspected that AOF/EMS products would be more prolific in larger organisations, we sorted the information from largest to smallest by the number of online terminals, and we selected the top 1200 for the mail-out. Twelve hundred sites were selected initially due to cost considerations for an initial mail-out and a follow-up mail-out. Moreover, a relatively low response rate of even 10 percent would yield 120 usable responses.

The survey consisted of three sections and was accompanied by a cover letter. An appendix was also included in the survey in order to explain common EMS functionality. In total the survey was five pages long (excluding the cover letter). The cover letter explained the objectives of the study. *Section A* collected demographic data. This section included a number of questions regarding the technical environment (i.e. hardware, operating systems, networks, applications etc.) as well as data pertaining to the characteristics of the organization (i.e. number of personnel, number of workstations, annual revenue, type of industry, type of organisation etc.). *Section B* collected data pertaining to the use of EMS products. This section was composed of questions that can be divided into three separate sets. The first set of questions sought to identify the types of EMS products used, the level of privilege at which the EMS was running and the EMS functionality that was being utilised. In order to collect data on EMS functionality, the respondents were presented with 18 numbered EMS capabilities that were explained in the appendix section of the survey. For each capability, the respondents were asked to circle the corresponding number of the EMS capability that was being utilized in their organization. Additionally, space was provided for any other utilised functionality that was not listed in the appendix. The second set of questions in *section B* was designed to identify if input parameter settings and script languages were being utilised. Questions relating to the access restrictions over the scripts/parameters, as well as who was responsible for their development or maintenance, were also a part of this set of questions. The last set of questions in *Section B* dealt with identifying what change controls were applied to the modification of the scripts/parameters as well as what backup and recovery procedures were in place in case of failure (and if these procedures were documented and tested). Additionally, *section B* asked respondents to identify any other control issues that they felt were of concern in their environment. Such concerns, for example, could be problems with lack of standards, lack of documentation or lack of qualified staff. *Section C* allowed contact details for the summarised results of the study.

The survey was piloted with eight industry practitioners who were involved with the installations and maintenance of AOF/EMS systems within organisations in the local area. Issues of clarity of meaning of terms and ambiguity in question construction were identified and resolved. The final instrument was modified to reflect the resolution of these identified issues.

Clearly, the major contribution of this paper is therefore based on the data gathered through the questions in *section B,* which related to the actual use of EMS products in the respondents' organisations. The responses to the questions in this section allowed us to not only collect information on EMS usage and controls in place over EMS, but also identify other issues that may be relevant. In order to store and analyse the results of the survey, a database was implemented. Each of the responses in the returned surveys was codified and stored in the database.

[1] A copy of the survey is available from the authors on request.

5 SURVEY RESULTS AND DISCUSSION

The survey was sent out to the CIOs of 1200 organisations in late 2002. It was anticipated that the CIOs would not fill-out the survey, rather, that if they wanted their organisation to participate in the study, they would refer the survey to the relevant IS staff member. After a three week period, some 200 surveys had been returned due to such reasons as the addressee no longer known at the company or a company policy of not responding to surveys. Furthermore, the response to that point had been very poor. Accordingly, we performed a complete mail-out again to the remaining 1000 organisations with a letter imploring CIOs for a response even if it was that their organisation was not interested or involved with EMS systems. After a further three weeks, only 83 surveys had been returned. As a last measure, we selected 100 organisations from the non-respondents and attempted to contact them personally to ascertain if there were any systemic reasons for the non-response. This process proved to be ultimately fruitless as, in most cases, having contacted the organisation, they either had no recollection of receiving the survey or we could not determine the officer to whom the survey had been referred for action. Accordingly, we achieved finally a response rate of 8.3 percent. Such a response rate figures below the acceptable range for mail surveys of homogeneous groups, *viz*., 15 to 50 percent, as reported by Wallace and Mellor (1988).

While the response rate for the survey was seen as very low and was, in general, disappointing, the lack of responses can to a degree be seen as an indication of the lack of EMS awareness in Australian organisations. This indication is supported by the data collected through the returned surveys. Only 39 of the 83 respondents (47 percent) indicated that the organisation for which they worked was utilising EMS products to any degree. Clearly, organisations that do not utilise EMS, or that are not aware of EMS or its capabilities, would be less likely to return the surveys when compared to organisations currently utilising, or planning to utilise, EMS.

The breakdown of survey respondents by the size of organization for which they work is shown in Figures 2 and 3. The size of the organization can be judged by the number of employed personnel as well as by the annual revenue of the organization. Accordingly, Figure 1 illustrates the breakdown of respondents by the number of employed personnel, while Figure 2 illustrates the breakdown of respondents by the annual revenue (in millions Aud$) of the organisation for which they work. Forty-seven percent of respondents indicated they worked for organizations employing between 500 and 5000 people (20.5 percent working in organisation with between 500-999 employees, 26.5 percent working in an organization with between 1000-4999 employees), indicating medium-sized corporations. Accordingly, thirty-nine percent of respondents indicated that their organization's annual revenue was between Aud$100M and Aud$999M. Therefore, we can assume that almost half of the respondents worked for mid-sized organizations.

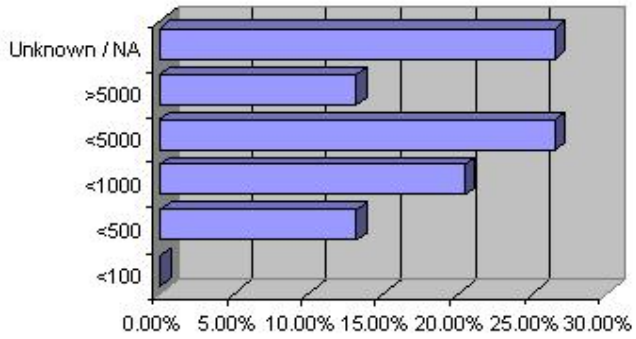

Figure 2. Size of responding organizations (measured by personnel).

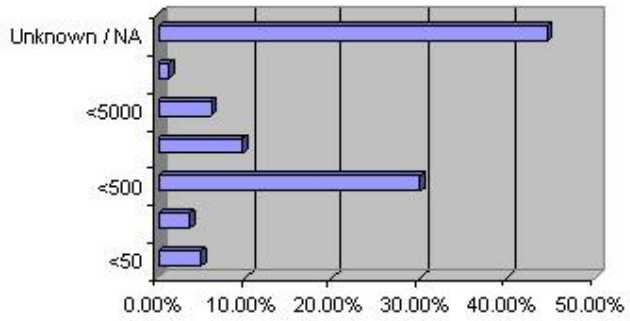

Figure 3. Revenue classification (in millions) of responding organisations.

We were interested in obtaining data in four areas related to EMS operation, *viz.*, extent of EMS usage, most frequently utilised functional capabilities of EMS, controls that are exercised over EMS, and what critical issues arise when an organisation uses EMS.

According to the data collected through the administration of the survey, almost half of the respondents indicated that the organisation for which they work utilised AOF/EMS to some extent. Of those respondents, thirty-nine percent indicated that BMC Patrol was being used within their organisation. The next most commonly used end-to-end EMS product was HP Openview, which was being utilised in 13 percent of the 39 respondents' organizations. The top six utilised end-to-end EMS products are shown in Table 1.

EMS Product	Response (N=39)	%
BMC Patrol	12	39
HP Openview	4	13
IBM Tivoli	3	10
CA Unicentre	3	10
SoPHOS	3	10

Table 1. Top 6 utilized end-to-end EMS products.

It has to be noted that not all organisations that utilise EMS do so with off-the-shelf products. Fifteen percent of the 39 respondents indicated that the organization for which they work uses exclusively in-house developed EMS products while 2.5 percent utilise a mix of off-the-shelf and in-house developed products. A further 5 percent indicated that they rely on a third-party, and the third party's product choice, to monitor the operation of their servers.

Figure 4 demonstrates the relative level of privilege at which the installed products were allowed to run in the responding organisations. The level of privilege relates to the priority of execution that the operating system will assign to various software applications executing at any point in time, *i.e.*, the ability of the EMS to pre-empt execution of other critical production systems. The survey results showed that, of the respondents who indicated EMS usage within their organisation, 41 percent were running EMS with the highest level of privilege. Only 5 percent of the applicable respondents indicated EMS use at a medium privilege level, while 31 percent indicated they used EMS for monitoring purposes only (low level of privilege). A further 18 percent of applicable respondents

indicated that while EMS was in place, it was not being utilised to monitor automatically or control the operation of the organisation's servers.

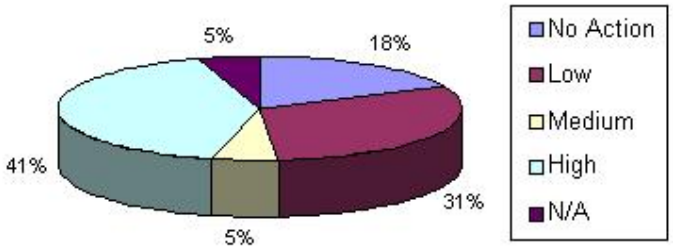

Figure 4. EMS levels of privilege.

In answering the question relating to the utilised EMS capabilities, 64.1 percent of respondents indicated that EMS was, in some form, used for operating system management. Fifty-six percent of respondents also indicated that EMS was being used for standard reporting, including system performance metrics. Almost fifty-four percent of respondents indicated that the user notification system was being used. These three EMS functionalities were reported to be the most commonly used. Among other commonly utilised functionalities were: automatic detection of applications databases and hardware environment (48.72 percent), and, production monitoring (41.03 percent). Meanwhile, the least commonly utilised EMS capabilities were: resource accounting and charging (7.69 percent), standardised text editor to produce system specific JCL within a script language (7.69 percent) and output management (10.26 percent). The full list of EMS capabilities and their respective frequency of utilisation are shown in Table 2.

Utilized capability	Response (N=39)	%
Operating system management	25	64.10%
Standardized reporting	22	56.41%
User notification system	21	53.85%
Automatic detection	19	48.72%
Production monitoring	16	41.03%
Database management	12	30.77%
Network management	12	30.77%
Graphical presentation	11	28.21%
Storage management	11	28.21%
Internet monitoring	10	25.64%
Job restart	9	23.08%
Application management	9	23.08%
Virus scanning	8	20.51%
Job flow and workload management	8	20.51%
Security management	6	15.38%
Output management	4	10.26%

Standardized text editor	3	7.69%
Resource accounting and charging	3	7.69%
Other	1	2.56%

Table 2. Utilised EMS functionality.

In relation to the use of input parameters and script languages, 66.6 percent indicated the use of parameter settings with the organisation's EMS product while 71.8 percent indicated the use of a script language. In both cases, the indication is that the system specialist is responsible for the development of scripts (78.6 percent) and the maintenance of parameter settings (73.1 percent) as seen in Table 3. Therefore, we can conclude that there is adequate security over scripts and parameters as well as adequate expertise in their maintenance/development. Approximately four percent indicated that there is no person in their organisation responsible for such maintenance or development.

Scripts developed by:	Response (N=28)	%	Parameter Settings Maintained By:	Response (N=26)	%
Systems Specialist	22	78.57%	Systems Specialist	19	73.08%
Operations	3	10.71%	Operations	7	26.92%
Nobody	1	3.57%	Nobody	1	3.85%
Not specified	2	7.14%	-	-	-

Table 3. Responsibilities for development of scripts and maintenance of parameters.

Access control for scripts was seen to be adequate, with only 3.6 percent indicating that no access control was in place (see Table 4). Over 71 percent of respondents indicated that access to scripts was controlled via the operating system while in 10.7 percent of the cases, access was controlled by third-party security software.

Access control for scripts	Response (N=28)	%
Operating System	20	71.43%
Third party security software	3	10.71%
Password	0	0.00%
None	1	3.57%
Not specified	4	14.29%

Table 4. Implemented access controls for scripts.

The last two areas of interest in this study were the identification of controls in place over the EMS as well as any additional issues that arose in the organisation as a result of EMS usage.

In general, looking at Table 5, change controls appear to be moderately low in usage, with independent testing being the lowest in use (only 30 percent). However, while Table 5 shows the data for individual change controls, according to "best practice", application of *all* change controls should occur. However, only 16 percent of the 37 respondents indicated that the organization applied all of the six listed change controls. Almost 19 percent indicated that only one of the listed change controls was being applied, two were applied in 13 percent of the cases, three were applied in 16 percent of the

cases, four in 10 percent of the cases and five of the listed change controls were applied in almost 19 percent of the cases.

Change controls	Response (N=37)	%
Authorisation	23	62.16%
Separate development environment	24	64.86%
Unit testing	20	54.05%
Independent testing	11	29.73%
Updating script documentation	18	48.65%
Controlled release to production	20	54.05%
OTHER	1	2.70%

Table 5. Utilised change controls in modification of scripts/parameters.

In terms of backup procedures for scripts and parameters, almost seventy-one percent of the 37 respondents indicated that the backup for scripts and parameters was incorporated in regular system backups (Table 6). Almost nineteen percent indicated that separate backups are used. Therefore over eighty-nine percent of respondents indicated scripts and parameter settings as backed up while 10.81 percent indicated no backup procedures. Additionally, 72.97 percent of applicable respondents indicated that the backup procedures were documented.

Backup procedures	Response (N=37)	%
Regular system backups	26	70.27%
Separate backups	7	18.92%
No backup procedures	4	10.81%
Procedures are documented	27	72.97%

Table 6. Backup procedures for scripts/parameters.

A similar situation was found to exist with the recovery procedures for scripts and parameters (Table 7). Over 86 percent of the applicable respondents indicated that recovery procedures were in place - slightly lower than that for the data on backups, but overall adequate. The recovery procedure documentation data were also lower, with 62 percent indicating recovery procedures were documented. Additionally, 65 percent of the 37 respondents indicated that the recovery procedures are tested periodically.

Recovery procedures	Response (N=37)	%
System recovery procedures	26	70.27%
Separate recovery procedures	6	16.22%

No recovery procedures	5	13.51%
Procedures are documented	23	62.16%
Tested periodically	24	64.86%

Table 7. Recovery procedures for scripts/parameters.

There were several additional control issues that were discovered as a result of this study. These issues are shown in Table 8 below. Of the identified issues, mutliskilling staff and availability of skilled staff were the most frequent control issues (46 percent) that organisations utilising EMS products faced.

Identified Issue	Response (N=39)	%
multiskilling staff	11	28.21%
lack of qualified/motivated staff	4	10.26%
outsourcing due to lack of skilled staff	3	7.69%
pace of technology/business change	2	5.13%
separation of duties	1	2.6%
lack of EMS products	1	2.6%
ongoing commitment to monitoring and controlling systems	1	2.6%
ensuring standards are maintained	1	2.6%
ensuring documentation is maintained	1	2.6%
ensuring untested scripts are not released	1	2.6%

Table 8. Additional identified issues.

The results of the survey appear to be supported to a certain extent by the those of the qualitative study performed by Green and Best (2003). Table 9 shows the results of this survey according to the issues used in the Green and Best (2003) study and provided in Figure 1.

Control Issues	Response (N=39)	%	Rating*	Green & Best (2003)**
Authorisation				
• Authorisation	22	56.4	Med	Lo

• Standards	19	48.7	Lo	N/A
Documentation	31	79.5	Med-Hi	Lo
Backups	32	82.1	Hi	Hi
Separation of Duties	10	25.7	Lo	Lo
Contingency Plans	31	79.5	Med-Hi	Med
Security				
• Scripts	23	59%	Med	Hi
• Parameters	23	59%	Med	Hi
Program Change Controls	28	71.8%	Med	Lo

Table 9. Control issues recognised by organisations utilising EMS.

(* 0-40 percent = Lo, 41-79 percent = Med, 80-100 percent = Hi)

(1-2 cases = Lo, 3 cases = Med, 4-5 cases = Hi)**

As Table 9 demonstrates, organisations implementing AOF/EMS appear to pay little attention to the control issues of separation of duties (*i.e.*, different people/groups developing, maintaining, and migrating scripts/parameters) and producing/changing scripts according to organisational standards. Furthermore, mediocre attention is paid to the implementation of change controls for scripts, establishing/maintaining scripts and parameters in secure libraries, and establishing/maintaining authorisation procedures for the production/changes to scripts. By contrast, significant attention is paid to the establishment of backup procedures for the scripts, contingency plans in the event the EMS fails and interrupts the operation of the entire production system, and documentation about the scripts and their use. In addition, to these *a priori* control issues, Table 8 tells us that multiskilling staff, a lack of qualified/motivated staff, outsourcing due to a lack of internally qualified staff, and the pace of technology/business change that influence the systems we are attempting to control, are the top four issues that respondents believe also need to be controlled in the implementation of AOF/EMSs.

There is some triangulation agreement between the qualitative results of Green and Best (2003) and the results of this study. The importance of script backups and contingency plans, and the virtual absence of separation of duties, were issues upon which both studies appear to align. In terms of scripts and parameters, access controls for scripts were found to be adequate in the interviewed organizations, as was found in the case of the survey data. Similarly, change controls applied in the interviewed organisations were found to range from nonexistent to adequate, while the survey data indicated a range between nonexistent and very good.

The data obtained from the interviews indicated that EMS products were being run at either high or monitoring-only privilege levels, a characteristic that was also apparent in the data collected through the survey (see Figure 4). Moreover, the pattern of EMS capability usage in the interviewed organisations was similar to that discovered through the application of the survey. The interview data indicated that the most utilised capabilities were: automatic detection (100%), operating system management (100%), database management (100%) and standardised reporting (80%). Of these capabilities, three are in the top-four utilised capabilities as indicated by the survey data (see Table 2). Of the additional identified issues during the interviews, adequate level of expertise in the software (3 cases) and the lack of qualified backup staff (2 cases) were the most commonly raised concerns. By contrast, Table 8 tells us that multiskilling staff, a lack of qualified/motivated staff, outsourcing due to a lack of internally qualified staff, and the pace of technology/business change that influence the

systems we are attempting to control, are the top four issues that respondents believe also need to be controlled in the implementation of AOF/EMSs.

6 SUMMARY, LIMITATIONS, AND CONCLUSIONS

This paper reported the results of a survey conducted in 2002 on the usage of EMS products within organisations. Unfortunately, due to the apparent immaturity of the AOF/EMS market in Australia in particular (and, we suspect, organisational "survey fatigue"), we could obtain only a response rate of 8.3 percent. However, the study found that 47% of respondents work for organisations currently utilising EMS products. It was also discovered that the most popular end-to-end EMS products were BMC Patrol, HP Openview and IBM Tivoli. In addition, the survey has shown that the most frequently utilised EMS capabilities were operating system management, standardised reporting, user notification system, as well as the automatic detection of applications, databases and hardware environment. Furthermore, the study found that while security controls over scripts as well as backup and recovery procedures tend to be adequate, change controls applied to the modification of scripts/parameters ranged from nonexistent to very good. In terms of the additional issues that are introduced when an organisation utilizes EMS products, the most common concerns identified in this study relate to the multiskilling of staff, a lack of qualified/motivated staff, outsourcing due to a lack of internally qualified staff, and the pace of technology/business change that influence the systems we are attempting to control. Multiskilling of staff as well as the availability of qualified staff are issues that are consistent with those uncovered through a previous study (Green & Best, 2003) that involved in-depth interviews/case studies of five organisations.

Apart from the usual limitations of surveys, *viz.*, incentives to respond, responding by saying what you hope you are doing rather than what you are actually doing in the organisational context, the survey being filled out by the appropriate person, one of the main limitations of this study was the low response rate (8.3 percent). Despite significant attempts by the researchers, the response rate was disappointing. Such a low response rate was seen as an indication of the lack of utilization, or lack of awareness, of EMS products (and, perhaps, "survey fatigue" in organisations). Additionally, this study suffers from a lack of generalisability of the results to other organisations as well as potential subjectivity in the classification of comments.

For organisations looking to implement AOF/EM systems, our results imply that they should focus their controls first and foremost on the establishment of backups, contingency plans, and documentation. They should then turn to the establishment of authorisation procedures, security over the storage of scripts/parameters, and script change controls. Organisations must ensure that they have appropriate staff skilled in the use of the product. Moreover, they should ensure that they multiskill staff to provide backup knowledge on the use/maintenance of such products. If organisations chose, because of a lack of internal expertise, to outsource the running of such systems for their computing operations, then they must consider compensating controls such as external independent review of the outsourcer. For the academic and practitioner literatures, this study provides some empirical support for the new types of controls required in computer operations environments run by AOF/EMS products. Furthermore, it extends the system of controls prescribed by Weber (1999), King (1990), and the CISA Review Manual (2004) to include such issues as the multiskilling of staff, a lack of qualified/motivated staff, outsourcing due to a lack of internally qualified staff, and the pace of technology/business change that influence the systems we are attempting to control.

References

Ayers, S. and Fentress, D. (2000) "Enhancing IT Governance Through Enterprise Management Software Solutions", *Information Systems Control Journal*, Vol. 2, pp. 1-5.

Bae, B., Epps, R., and Gwathmey, S. (2003) “Internal Control Issues: The Case of Changes to Information Processes”, *Information Systems Control Journal*, Vol. 4, pp. 44-46.

Certified Information Systems Auditor Review Manual (2004), Information Systems Audit and Control Association (ISACA): Rolling Meadows.

Garvey, M. (1999) “Storage Gains Flexibility”, *Informationweek*, No. 754, p. 30.

Gisinger, A., Shankaran, R. and Ray, P. (2001) “An evaluation process for enterprise management systems: a business perspective”, Proceedings of *2001 Enterprise Networking, Applications, and Services Conference*, pp. 9-16.

Green, P. and Best, P. (2003) ”Information Systems Audit and Control Issues for Enterprise Management Systems: Some Qualitative Evidence”, Accounting and Finance Association of Australia and New Zealand Conference, Brisbane, July.

Greenstein, I. (1992) “Quit babysitting your LANs”, *Networking Management*, No. 3, pp. 70-75.

Hagendorf-Follett, J. (2001) “Serving the Enterprise”, *Computer Reseller News*, No. 928, p. 100.

Johnston, M. (2001) “IBM Systems Management Software Predicts Server Failure”, *InfoWorld*, Vol 23, No. 5, p. 20.

King, J. (1990) “Auditing the lights-out facility”, *EDPACS*, Vol. 18, No. 3, pp. 1-8.

Lais, S. (2000a) “BMC’s Patrol Targets B2B Management”, *Computerworld*, Vol. 34, No. 33, p. 52.

Lais, S. (2000b) “HP Launches OpenView Suite that offers Business View”, *Computerworld*, Vol. 34, No. 6, p. 10.

Marlin, S. (1999) “Enterprise Systems Management: Banks look to get a grip on IT”, *Bank Systems & Technology*, Vol. 36, No. 11, pp. 42-48.

Middlemiss, J. (2000) “ABN AMRO taps Computer Associates’ Platform to Consolidate Disparate Systems”, *Bank Systems & Technology*, Vol. 37, No. 9, p. 24.

Miller, H.W. (1988) “Planning for unattended data center operation”, *Mainframe Journal*, Jan/Feb., pp. 10-15.

Mullen, J. (1993) “Auditing the Data Center: Setting audit test objectives”, *EDP Auditing*, Auerbach Publications, pp. 1-15.

Saunders, J. (1999) “CA adds Storage Control to its Management Tools”, *Computing Canada*, Vol. 25, No. 28, p. 23.

Songini, M. (2000) “CA targets Quality of Service, Service-Level Management”, *Network World*, Vol. 17, No. 14, p. 10.

Sprague, R. and McNurlin, B. (1993) *Information Systems Management in Practice*, Prentice-Hall:Englewood-Cliffs.

Wallace, R. S. And Mellor, C.J. (1988) ”Nonresponse bias in mail accounting surveys: A pedagogical note”, *The British Accounting Review*, Vol. 20, No. 2, pp. 131-139.

Weber, R. (1999) *EDP Auditing: Conceptual Foundation and Practice*, 3rd edn., Prentice-Hall:New Jersey.

Yasin, R. (1999) “BullSoft combines Security, Management”, Internetweek, No. 766, p. 8.

Yasin, R. (2000) “Anticipate Problems, Map Changes – Software that Sees the Future”, *Internetweek*, No. 827, p. 1.